ABSTRACT

An encryption method in which a clear message (m) is formatted with a formatting function (μ), and in which the result of the formatting step is exponentiated using a public key (N, e) in accordance with the relationship $c = \mu(m)^e \bmod N$, c being an encrypted message, μ(m) being the result of the formatting step, and e and N elements of the public key. The formatting function (μ) is the PSS function. The invention is applicable to cryptography, for example of RSA type, for smart cards for instance.